EP/EP2004 4 7 0 0 5 1 9 1

BUNDESREPUBLIK DEUTSCHLAND

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen: 103 14 559.1

Anmeldetag: 31. März 2003

Anmelder/Inhaber: Siemens Aktiengesellschaft,
80333 München/DE

Bezeichnung: Verfahren und Steuerungsprogramm zum Betrieb eines Kommunikationsendgeräts für paketorientierte Datenübermittlung

IPC: H 04 L 9/32

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 29. Januar 2004
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Hintermeier

A 9161
08/00
EDV-L

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

Beschreibung

Verfahren und Steuerungsprogramm zum Betrieb eines Kommunikationsendgeräts für paketorientierte Datenübermittlung

Das Internet-Protokolls (IP) zur paketorientierten, verbindungslosen Datenübertragung wird nicht nur für einen reinen Datentransfer verwendet. Auch für Sprach- und Bildsignalübertragung ist eine Verwendung des Internet-Protokolls wegen zunehmender Installation IP-basierter Netze, wie Intranets und Extranets, eine interessante und kostengünstige Alternative zu herkömmlichen Kommunikationsstrukturen. Die Sprachsignalübertragung mittels des Internet-Protokolls, Voice-over-IP (VoIP), konkurriert insbesondere mit klassischen, verbindungsorientierten Sprachnetzen. Für die Nutzung des Internet-Protokolls zur Sprachsignalübertragung ist sein Echtzeitverhalten von zentraler Bedeutung. Das Echtzeitverhalten wird durch die Minimierung von Datenpaketverlusten und Verzögerungszeiten bestimmt, zumal Anwender bei der Sprachsignalübertragung nur minimale Verzögerungen akzeptieren.

Entscheidend für eine Akzeptanz von Voice-over-IP wird auch eine Einbindung und Nutzung von vorhandenen Telekommunikationssystemen sein. Auf Anwenderseite besteht nämlich großes wirtschaftliches Interesse an einer Weiternutzung bisheriger, konventioneller Telekommunikationssysteme einschließlich aller gewohnten Leistungsmerkmale. Voice-over-IP ist als Ablösung für konventionelle Nebenstellentechnik geplant und bietet eine Basis für eine weitergehende Integration von Sprach-, Daten- und Video-Diensten, beispielsweise im Rahmen von Multimediakonferenzen, Application Sharing oder Call-Center-Anwendungen. Aufgrund einer Vereinheitlichung von Betriebsfunktionen für Daten und Sprache können Synergiepotentiale ausgenutzt werden. Darüber hinaus ermöglicht Voice-over-IP standardisierte Umgebungen mit Schnittstellen zu konventionellen Telekommunikationssystemen einschließlich öffentlichen Telekommunikationsnetzen.

Mögliche Anwendungsszenarien für Voice-over-IP in einem Intranet sehen standortgebundene IP-Telefon-Gateways vor, über welche Gespräche von einer Telekommunikationsanlage geleitet werden. Einem solchen Gateway kommt die Aufgabe zu, Signalisierung, Standardprotokolle sowie herstellerspezifische Protokolle zu unterstützen. Derzeit weist Voice-over-IP einschließlich einer Integration in bestehende Telekommunikationsanlage noch einige Schwachpunkte auf hinsichtlich Signalisierung, verfügbarer Leistungsmerkmale und geeigneter Netzmanagement-Systeme. Bei letzteren umfassen Anforderungen eine gesamtheitliche Überwachung und Verwaltung von bislang getrennter Sprach- und der Datenkommunikation.

In zahlreichen VoIP-Telefonnetzen halten VoIP-Endgeräte Daten über ihren Zustand in einem dem jeweiligen VoIP-Endgerät zugeordneten Speicher. Der Gerätezustand umfaßt beispielsweise Angaben wie Rufnummer, programmierte Tastenbelegungen oder aktivierte Leistungsmerkmale. Üblicherweise ist einem VoIP-Endgerät in VoIP-Telefonnetzen eine als Gatekeeper bekannte Steuerungseinheit zugeordnet, die beispielsweise ein Weitervermitteln von Rufsignalisierungen sowie ein Auflösen oder Umwandeln von Netzwerkadressen oder Telefonnummern wahrnimmt. In der Regel sind Gatekeeper daher vor allem für Zugangsberechtigungen und Sicherheitsaspekte vorgesehen. Zusätzlich können Gatekeepern auch Aufgaben im Bereich der Gebührenerfassung, -zuweisung oder eines Bandbreitenmanagements zur Gewährleistung einer vorgegebenen Dienstgüte zugewiesen werden.

Fällt ein Gatekeeper in einem VoIP-Telefonnetz aus, so sind insbesondere VoIP-Endgeräte betroffen, die dadurch ihre Zuordnung im VoIP-Telefonnetz verlieren. Ein Sicherheitsproblem stellt in diesem Zusammenhang eine Neuzuordnung der betroffenen VoIP-Endgeräte zu einem alternativen Gatekeeper dar, da die betroffenen VoIP-Endgeräte üblicherweise noch nicht durch den alternativen Gatekeeper registriert sind.

Der vorliegenden Erfindung liegt daher die Aufgabe zugrunde, ein Verfahren zum Betrieb eines Kommunikationsendgeräts für paketorientierte Datenübermittlung sowie effiziente Realisierung des Verfahrens anzugeben, das ein sicheres Neuzuordnen des Kommunikationsendgeräts zu einer alternativen Steuerungseinheit nach Ausfall einer zuvor zugeordneten Steuerungseinheit ermöglicht.

Diese Aufgabe wird erfindungsgemäß durch ein Verfahren mit den in Anspruch 1 angegegebenen Merkmalen und ein Steuerungsprogramm mit den in Anspruch 6 angegebenen Merkmalen gelöst. Vorteilhafte Weiterbildungen der vorliegenden Erfindung sind in den abhängigen Ansprüchen angegeben.

Ein wesentlicher Aspekt der vorliegenden Erfindung besteht darin, daß eine für ein Kommunikationsendgerät in einer zugeordneten Speichereinheit gespeicherte Zustandsinformation mit einer digitalen Signatur versehen wird. Die digitale Signatur wird aus der Zustandsinformation mittels eines privaten Schlüssels für ein asymmetrisches Verschlüsselungsverfahren berechnet, der einer dem Kommunikationsendgerät zugeordneten ersten Steuerungseinheit zur Auflösung bzw. Umwandlung von Netzwerkadressen zugeordnet ist. Bei einem Ausfall der ersten Steuerungseinheit wird eine die Zustandsinformation und die digitale Signatur umfassende Aufforderung zur Zuordnung des Kommunikationsendgeräts an zumindest eine zweite Steuerungseinheit übermittelt und die digitale Signatur verifiziert, beispielsweise durch die zweite Steuerungseinheit. Bei einem positiven Verifizierungsergebnis wird das Kommunikationsendgerät zur zweiten Steuerungseinheit zugeordnet. Auf diese Weise kann ein unberechtigtes Einschleusen eines VoIP-Endgeräts an einer zur Zuordnung vorgesehenen Steuerungseinheit, beispielsweise einem Gatekeeper, unterbunden werden.

Die vorliegende Erfindung wird nachfolgend an einem Ausführungsbeispiel anhand der Zeichnung näher erläutert. Es zeigt

Figur 1 eine schematische Darstellung eines Anwendungsumfeldes der vorliegenden Erfindung,

Figur 2 ein Ablaufdiagramm für ein Verfahren und Steuerungsprogramm zum Betrieb eines Kommunikationsendgeräts für paketorientierte Datenübermittlung.

Das in Figur 1 schematisch dargestellte Anwendungsumfeld der vorliegenden Erfindung umfaßt ein lokales Paketdatennetz 101, welches mehrere VoIP-Telefone 111-113, PC-basierte Kommunikationsendgeräte 121-122, Gatekeeper 131-133, einen Rooter 102 und ein Gateway 103 miteinander verbindet. Die VoIP-Telefone 111-113 und die PC-basierten Kommunikationsendgeräte 121-122 stellen Kommuniktionsendgeräte für paketorientierte Datenübermittlung dar, wobei die VoIP-Telefone 111-113 lediglich einer Sprachsignaübermittlung dienen.

Die Gatekeeper 131-133 sind als zentrale Steuerungselemente für ein Weiterleiten von Rufsignalisierungen sowie eine Auflösung bzw. Umwandlung von Telefonnummern und Netzwerkadressen vorgesehen. Außerdem erfassen die Gatekeeper 131-133 Gebühren und weisen sie Netzbenutzern bzw. Diensten zu. Für Voice-over-IP stellen die Gatekeeper 131-133 wichtige Komponenten dar, da auf ihnen Software für ein Management von Zonen und Rufdiensten installiert ist, die dort abläuft.

Der Rooter 102 ist als Koppelelement zwischen dem lokalen Paketdatennetz 101 und einem weiteren IP-basierten Netz 104, beispielsweise dem Internet, vorgesehen und verbindet das lokale, IP-basierte Paketdatennetz 101 das weitere IP-basierte Netz 104 auf der Vermittlungsschicht gemäß dem OSI-Referenzmodell miteinander. Vornehmlich nimmt der Rooter 102 Aufgaben im Bereich Protokollumsetzung und Datenratenadaption wahr.

Das Gateway 103 umfaßt Hard- und Software um verschiedenartige Netze miteinander zu verbinden. Im vorliegenden Fall wird durch das Gateway 103 ein öffentliches Telefonnetz 105 durch

Protokollumsetzung an das lokale, IP-basierte Paketdatennetz 101 angeschlossen. Das Gateway 103 hat insbesondere die Aufgabe, Nachrichten von einem Netz in ein anderes zu übermitteln, was vor allem eine Kommunikationsprotokolumwandlung erfordert. Ferner ist das Gateway 102 in der Lage, Protokolle vollständig aufzulösen, und stellt sowohl aus Sicht des öffentlichen Telefonnetzes 105 als auch aus Sicht des lokalen Paketdatennetzes 101 einen adressierbaren Netzknoten dar. Eine durch das Gateway 103 durchgeführte vollständige Protokollumwandlung umfaßt eine Umsetzung von Adressen und Formaten, eine Konvertierung der Codierung, eine Zwischenpufferung von Datenpaketen, eine Paketbestätigung, eine Flußkontrolle sowie eine Geschwindigkeitsanpassung.

Für jedes der Kommunikationsendgeräte 111-113, 121-122 werden Zustandsinformationen in einer Speichereinheit des jeweiligen Kommunikationsendgeräts gespeichert. Diese Zustandsinformationen umfassen beispielsweise Ruflisten, Umleitungen programmierte Tastenbelegungen oder aktivierte Leistungsmerkmale oder Mehrwertdienste. Die Zustandsinformationen werden dabei als Datencontainer in der jeweiligen Speichereinheit verwaltet und durch einen dem jeweiligen Kommunikationsendgerät 111-113, 121-122 zugeordneten Gatekeeper 131 bis 133 laufend aktualisiert. Die Abspeicherung der Zustandsinformationen entspricht 201 des in Figur 2 dargestellten Ablaufdiagramms, die Aktualisierung der Zustandsinformationen entspricht Schritt 210.

Ferner wird eine digitale Signatur generiert (Schritt 202) mit der die jeweiligen Zustandsinformationen versehen werden. Die digitale Signatur wird jeweils aus den in dem jeweiligen Speicher gespeicherten Zustandsinformationen mittels eines privaten Schlüssels für ein asymmetrisches Verschlüsselungsverfahren berechnet und gemeinsam mit den Zustandsinformationen in der jeweiligen Speichereinheit gespeichert. Die jeweilige digitale Signatur wird dabei mittels des privaten Schlüssels berechnet, der dem zum jeweiligen Kommunikations-

endgerät 111-113, 121-122 zugeordneten Gatekeeper 131-133 zugeordnet ist. Ein öffentlicher Schlüssel zur Verifizierung einer digitalen Signatur eines jeweiligen Gatekeepers 131-133 ist in den jeweils anderen Gatekeepern abrufbar hinterlegt. Im allgemeinen sind die öffentlichen Schlüssel so hinterlegt, daß diese für sämtliche Gatekeeper innerhalb einer IP-Telefonie-Domäne verfügbar sind.

Die laufende Aktualisierung der Zustandsinformationen spiegelt sich in Schritt 203, durch den abgefragt wird, ob eine Änderung von Zustandsinformation vorliegt, und in Schritt 210 wieder, durch den gegebenenfalls eine Zustandsinformation aktualisiert wird. Ein Ausfall eines einem Kommunitkationsgerät 111-113, 121-122 zunächst zugeordneten Gatekeepers 131 wird durch die vom Ausfall betroffenen Kommunikationsendgeräte festgestellt, wenn eine zyklische Aktualisierung von Zustandsinformtionen nicht mehr funktioniert. Dadurch sind die Kommunikationsendgeräte in der Lage, einen Ausfall eines Gatekeepers zu erkennen (Schritt 204).

Liegt ein Ausfall des zunächst zugeordneten Gatekeepers 131 tatsächlich vor, so übermitteln die von dem Ausfall betroffenen Kommunikationsendgeräte eine Meldung mit einer Aufforderung zur Zuordnung des jeweiligen Kommunikationsendgerätes an zumindest einen alternativen Gatekeeper 132-133. Die Meldung mit der Aufforderung zur Zuordnung der vom Ausfall betroffenen Kommunikationsendgeräte umfaßt die in den jeweiligen Kommunikationsendgeräten gespeicherten Zustandsinformationen einschließlich der digitalen Signatur. Vorzugsweise sollte in jedem Kommunikationsendgerät zusätzlich eine Liste mit alterantiven Gatekeepern abgespeichert sein, damit von einem Ausfall eines Gate-Keepers betroffene Kommunikationsendgeräte gleichverteilt einen alternativen Gatekeeper auswählen können. Auf diese Weise wird eine automatische Lastverteilung gewährleistet. Die Übermittlung der Meldung mit einer Aufforderung zur Zuordnung eines alternativen Gatekeepers ent-

spricht Schritt 205 des in Figur 2 dargestellten Ablaufdiagramms.

Der alternative Gatekeeper 132-133, der eine Meldung mit einer Aufforderung zur Zuordnung eines Kommunikationsendgerätes empfangen hat, verifiziert zunächst die von der Meldung umfaßte digitale Signatur (Schritt 206). Wenn die digitale Signatur beispielsweise aus einem für die Zustandsinformationen ermittelten Hash-Wert berechnet ist, wird zur Verifizierung der digitalen Signatur durch einen der alternativen Gatekeeper 132-133 für die von einem Kommunikationsendgerät übermittelten Zustandsinformation ein Hash-Wert berechnet und dieser mit einer mittels eines dem ausgefallenen Gatekeeper 131 zugeordneten öffentliche Schlüssels entschlüsselten digitalen Signatur auf Übereinstimmung verglichen. Zur Berechnung der digitalen Signatur kann beispielsweise ein Message-Diagest-No.5-Alghorithmus (MD5) verwendet werden. Zum Abschluß der Verifizierung der digitalen Signatur wird das Überprüfungsergebnis abgefragt, was sich in Schritt 207 des in Figur 2 dargestellten Ablaufdiagramms widerspiegelt.

Kann die digitale Signatur nicht erfolgreich verifiziert werden, so wird eine Neuzuordnung des jeweiligen vom Ausfall des zuvor zugeordneten Gatekeepers 131 betroffenen Kommunikationsendgerätes zu einem alternativen Gatekeeper 132-133 abgewiesen (Schritt 208). Bei einem positiven Verifizierungsergebnis wird das Kommunikationsendgerät zum jeweiligen alternativen Gatekeeper 132-133 zugeordnet (Schritt 209) und die Zustandsinformationen für das Kommunikationsendgerät gegebenenfalls aktualisiert (Schritt 210).

Das beschriebenen Verfahren zum Betrieb eines Kommunikationsendgerätes für paketorientierte Datenübermittlung kann beispielsweise in Form eines Steuerungsprogramms implementiert sein. Bei einer dezentralen Implementierung des Verfahrens sind in den Kommunikationsendgeräten Steuerungsprogramme installiert, die in einen Arbeitsspeicher eines jeweiligen PC-

basierten Kommunikationsendgeräts ladbar sind und Codeabschnitte aufweisen, bei deren Ausführung die vorangehend beschriebenen Schritte durchgeführt bzw. veranlaßt werden, wenn das jeweilige Steuerungsprogramm im jeweiligen PC-basierten Kommunikationsendgerät abläuft. Schritte zur Verifizierung einer digitalen Signatur und zur Zuordnung eines neuen Gatekeepers können durch in den alternativen Gatekeepern installierte Steuerungsprogramme durchgeführt werden.

Die vorliegende Erfindung ist nicht auf das hier beschriebenen Ausführungsbeispiel beschränkt.

Patentansprüche

1. Verfahren zum Betrieb eines Kommunikationsendgeräts für paketorientierte Datenübermittlung, bei dem

- für ein Kommunikationsendgerät zumindest eine Zustandsinformation in einer dem Kommunikationsendgerät zugeordneten Speichereinheit gespeichert wird,
- die Zustandsinformation mit einer digitalen Signatur versehen wird, die aus der Zustandsinformation mittels eines privaten Schlüssels für ein asymmetrisches Verschlüsselungsverfahren, der einer dem Kommunikationsendgerät zugeordneten ersten Steuerungseinheit zur Auflösung und/oder Umwandlung von Netzwerkadressen zugeordnet ist, berechnet wird,
- bei einem Ausfall der ersten Steuerungseinheit eine die Zustandsinformation und die digitale Signatur umfassende Aufforderung zur Zuordnung des Kommunikationsendgeräts an zumindest eine zweite Steuerungseinheit übermittelt und die digitale Signatur verifiziert wird,
- bei einem positiven Verifizierungsergebnis das Kommunikationsendgerät zur zweiten Steuerungseinheit zugeordnet wird.

2. Verfahren nach Anspruch 1,
bei dem die zumindest eine Zustandsinformation auf Veranlassung durch die erste oder zweite Steuerungseinheit zu einem vorgebbaren Zeitpunkt aktualisiert wird.

3. Verfahren nach einem der Ansprüche 1 oder 2,
bei dem die digitale Signatur aus einem für die Zustandsinformation ermittelten Hash-Wert berechnet ist.

4. Verfahren nach Anspruch 3,
bei dem zur Verifizierung der digitalen Signatur für die Zustandsinformation ein Hash-Wert berechnet und dieser mit einer mittels eines der ersten Steuerungseinheit zugeordneten

öffentlichen Schlüssels entschlüsselten digitalen Signatur auf Übereinstimmung verglichen wird.

5. Verfahren nach einem der Ansprüche 3 oder 4, bei dem zur Berechnung der digitalen Signatur ein Message-Digest-No.5-Algorithmus verwendet wird.

6. Steuerungsprogramm zum Betrieb eines Kommunikationsendgeräts für paketorientierte Datenübermittlung, das in einen Arbeitsspeicher einer Recheneinrichtung ladbar ist und zumindest einen Codeabschnitt aufweist, bei dessen Ausführung

- für ein Kommunikationsendgerät zumindest eine Zustandsinformation in einer dem Kommunikationsendgerät zugeordneten Speichereinheit gespeichert wird,
- die Zustandsinformation mit einer digitalen Signatur versehen wird, die aus der Zustandsinformation mittels eines privaten Schlüssels für ein asymmetrisches Verschlüsselungsverfahren, der einer dem Kommunikationsendgerät zugeordneten ersten Steuerungseinheit zur Auflösung und/oder Umwandlung von Netzwerkadressen zugeordnet ist, berechnet ist,
- bei einem Ausfall der ersten Steuerungseinheit eine die Zustandsinformation und die digitale Signatur umfassende Aufforderung zur Zuordnung des Kommunikationsendgeräts an zumindest eine zweite Steuerungseinheit übermittelt und eine Verifizierung der digitale Signatur veranlaßt wird,
- bei einem positiven Verifizierungsergebnis eine Zuordnung des Kommunikationsendgeräts zur zweiten Steuerungseinheit veranlaßt wird,

wenn das Steuerungsprogramm in der Recheneinrichtung abläuft.

Zusammenfassung

Verfahren und Steuerungsprogramm zum Betrieb eines Kommunikationsendgeräts für paketorientierte Datenübermittlung

Zum Betrieb eines Kommunikationsendgeräts für paketorientierte Datenübermittlung wird für ein Kommunikationsendgerät zumindest eine Zustandsinformation in einer dem Kommunikationsendgerät zugeordneten Speichereinheit gespeichert. Die Zustandsinformation wird mit einer digitalen Signatur versehen, die aus der Zustandsinformation mittels eines privaten Schlüssels für ein asymmetrisches Verschlüsselungsverfahren, der einer dem Kommunikationsendgerät zugeordneten ersten Steuerungseinheit zur Auflösung und/oder Umwandlung von Netzwerkadressen zugeordnet ist, berechnet wird. Bei einem Ausfall der ersten Steuerungseinheit wird eine die Zustandsinformation und die digitale Signatur umfassende Aufforderung zur Zuordnung des Kommunikationsendgeräts an zumindest eine zweite Steuerungseinheit übermittelt und die digitale Signatur verifiziert. Bei einem positiven Verifizierungsergebnis wird das Kommunikationsendgerät zur zweiten Steuerungseinheit zugeordnet.

Figur 2

FIG. 1

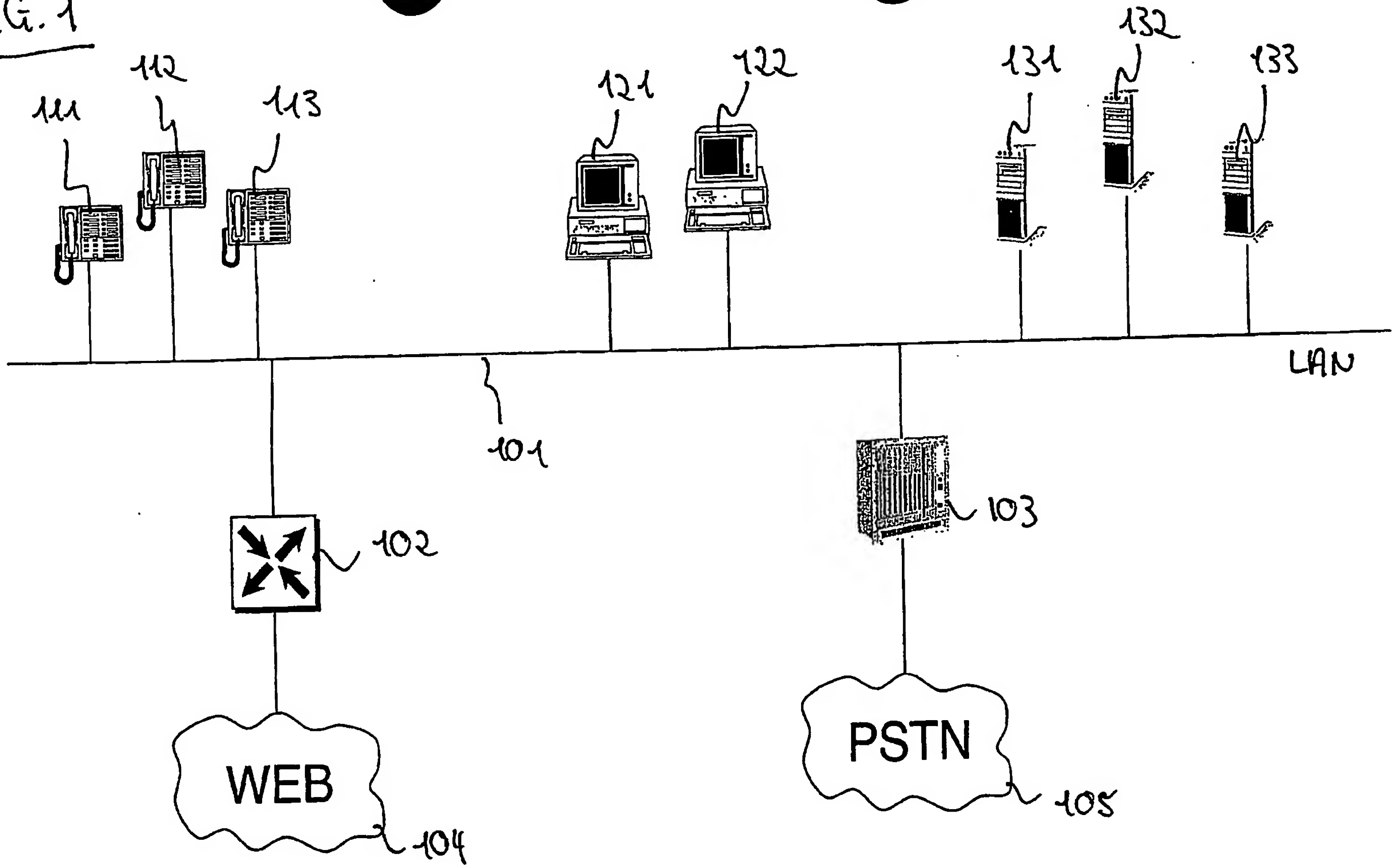
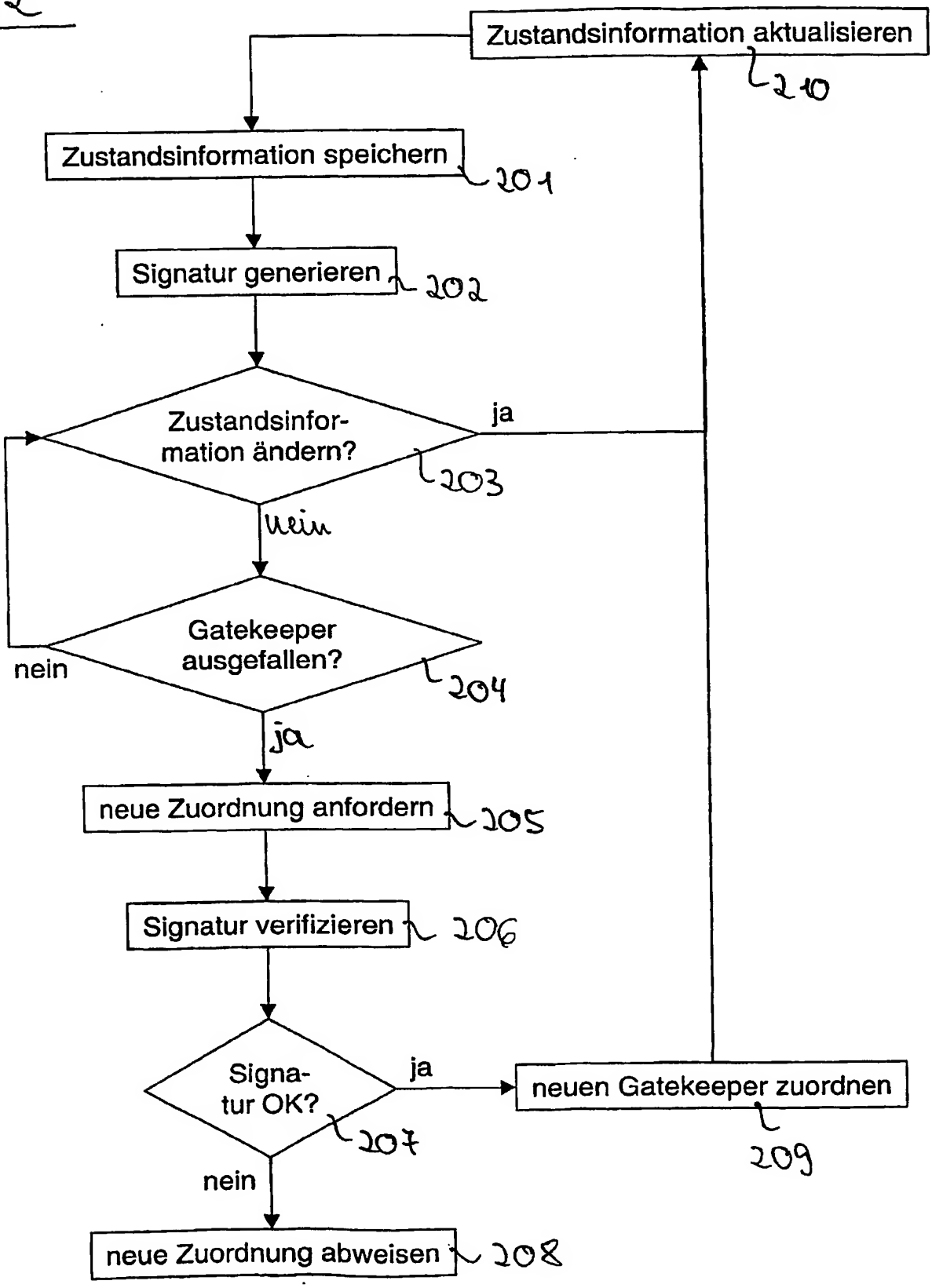


FIG.2


Zustandsinformation aktualisieren
210
Zustandsinformation speichern
201
Signatur generieren
202
Zustandsinformation ändern?
203
ja
nein
Gatekeeper ausgefallen?
204
nein
ja
neue Zuordnung anfordern
205
Signatur verifizieren
206
Signatur OK?
207
ja
neuen Gatekeeper zuordnen
209
nein
neue Zuordnung abweisen
208